A NOTE ON SHORT COSETS

ANDREAS-STEPHAN ELSENHANS[1]

Abstract. We describe some improved techniques for the computation of short cosets. This speeds up the computation of Galois groups in magma.

1. Introduction

The computation of Galois groups of polynomials with rational coefficients in modern computer algebra systems like magma [1] is based on the method of Stauduhar [10].

This method starts with an initial group G known to contain the Galois group (e.g., $G = \mathrm{Sym}(n)$). Then one computes the conjugacy classes of maximal subgroups of G. For each conjugacy class, one picks a representative $U \subset G$. By using a relative invariant [6, Def. 2.2] $I \in \mathbb{Z}[X_1, \ldots, X_n]$ for $U \subset G$, one can detect all the conjugates U^g of U that contain the Galois group. For more details and several improvements, we refer to [5], [6], and [7]. Further techniques for the construction of invariants are given in [4].

In the initial form, all the conjugacy classes of $U \subset G$ have to be tested. In [6, Sect. 5.2], the idea of short cosets was introduced. The starting point of this is that the Stauduhar method works with complex or p-adic root approximations. In the p-adic case p is an unramified prime. The local Galois group (generated by complex conjugation or by the Frobenius) is a subgroup of the (global) Galois group we are looking for. We denote by G_p the local subgroup generated by the Frobenius element f_p. Thus, one is interested in the *short cosets*

$$G//_{G_p}U := \{g \in G//U \mid G_p \subset U^g\}\,.$$

Here, $G//U$ denotes a set of coset representatives of G/U. The direct computation of the short cosets by the definition is only practical when the index of $U \subset G$ is small enough for a complete enumeration of the transversal. In practice, we do it this way for subgroups of index up to 10000.

2. A method to compute short cosets

A faster way to compute the short cosets is given in [6, Algorithmus 5.12]. It works as follows:

- Compute a list of representatives for the conjugacy classes of U.
- For each representative r, test whether it is conjugate in G to the generator of G_p. I.e., look for an element $g \in G$ such that $g^{-1} f_p g = r$.
- In case such a g exists it contributes $\{ag : a \in C_G(f_p)//C_{gUg^{-1}}(f_p)\}$ to the short cosets.

[1]Andreas-Stephan Elsenhans, School of Mathematics and Statistics F07, University of Sydney NSW 2006, Australia, andreas-stephan.elsenhans@sydney.edu.au

Here, $C_U(g)$ denotes the centralizer of g in U.

One obvious improvement is the use of homomorphisms. In case we have a homomorphism $\phi\colon G \longrightarrow H$ such that $\mathrm{Kern}(\phi) \subset U$, we can solve the short coset problem for $\phi(U) \subset \phi(G)$ with the known subgroup $\phi(G_p)$. To get the short cosets we are looking for, we take arbitrary preimages of the representatives found.

Remark. In practice, the limiting bottleneck of the method is the computation of the conjugacy classes of U. In particular, if U is an intransitive or an imprimitive group this can get slow. The point is that the orders of proper primitive groups are never that big [3, Chap. 5].

The test of conjugacy of elements in permutation groups is done in MAGMA by the method described in [9]. It is completely sufficient for the groups, we have to deal with.

3. Some examples and heuristics

In [6, Beispiel 5.9], the example of the primitive group $\mathrm{PSL}_2(\mathbb{F}_p) \subset \mathrm{Alt}(p+1)$ of index $(p-2)!$ is given. In case the known subgroup is the cyclic group of order $(p+1)$, we get only one short coset. Thus, in this case the improvement is huge.

A naive statistical estimate would be as follows. A random element of G is contained in U with probability $\frac{1}{[G:U]}$. If one assumes the elements f_p^g to be uniformly distributed in G then one expects to find one short coset, independently of the index of the subgroup.

Of course, this heuristic is very coarse. E.g., in case f_p is the identity, cosets and short cosets coincide. In case U is normal in G, we have either zero or $[G:U]$ short cosets. Note that maximal normal subgroups are not that problematic as their index is bounded by the degree of the permutation group.

An example where the short cosets do not work that well, independently of the choice of the known cyclic subgroup, is given by $G := \mathrm{PSL}_3(\mathbb{F}_4) \subset \mathrm{Alt}(56)$. Let us assume a polynomial with this Galois group is given. Then the Stauduhar method will inspect the maximal subgroups of the alternating group $\mathrm{Alt}(56)$. A double-cover G_1 of G of index $\frac{55!}{1440} \approx 8.8 \cdot 10^{69}$ will be found in $\mathrm{Alt}(56)$ as the only maximal subgroup class that may contain the Galois group. In this case it is impossible to pick a cyclic subgroup of G that results in less than $16602626880 \approx 16 \cdot 10^9$ short cosets for $G_1 \subset \mathrm{Alt}(56)$. In the `GAP` and MAGMA databases of primitive groups [2] G and G_1 are available via `PrimitiveGroup(56,1)` and `PrimitiveGroup(56,4)`.

In an initial step the Galois group algorithm chooses the prime p and the p-adic splitting field, it works with. By Chebotarev's density theorem, it can choose the known subgroup out of all cyclic subgroups of the Galois group. At this point, the question for a good prime selection strategy arises. It should be based on an expectation for the number of short cosets, we have to deal with.

The algorithm above gives a rough idea for this. If we assume that there are not too many conjugacy classes in U then we have to minimize $[C_G(f_p) : C_{gUg^{-1}}(f_p)]$ as we want to minimize the number of short cosets. If we estimate $\#C_G(f_p)$ by $\#C_{\mathrm{Sym}(n)}(f_p)$ and $\#C_{gUg^{-1}}(f_p)$ by $\#G_p$, we get an idea how many short cosets will be there.

It turns out to be a good prime choosing strategy to pick a prime such that this estimate is small.

4. The new method

Lemma. Let $G_p, U_0 \subset G_0$ be two subgroups and $\phi\colon G_0 \to H$ be a homomorphism such that $\phi(U_0) = \phi(G_0)$. We denote by G the subgroup $\phi^{-1}(\phi(G_p)) = \langle G_p, \mathrm{Kern}(\phi)\rangle$ and put $U := U_0 \cap G$. Then short cosets for $U \subset G$ with known subgroup G_p are short cosets for $U_0 \subset G_0$ with known subgroup G_p.

$$\begin{array}{ccccccccc} G_p & \subset & G & = & \phi^{-1}(\phi(G_p)) & \subset & G_0 & \overset{\phi}{\twoheadrightarrow} & H \\ & & \cup & & & & \cup & \nearrow & \\ & & U & = & G \cap U_0 & \subset & U_0 & & \end{array}$$

Remark. One can think of $G = \phi^{-1}(\phi(G_p)) = \langle G_p, \mathrm{Kern}(\phi)\rangle$ as the smallest subgroup of G_0 that contains G_p and can be defined using ϕ.

Proof of the lemma. Let gU_0 be a coset of $U_0 \subset G_0$. Then $\phi(g) \in \phi(G_0) = \phi(U_0)$. Thus, there is an element $u \in U_0$ such that $\phi(g) = \phi(u)$. Now, g and gu^{-1} represent the same U_0-coset. As $gu^{-1} \in \mathrm{Kern}(\phi) \subset G$, we see that each coset G_0/U_0 can be represented by an element of G. From now on, we assume all coset representatives of G_0/U_0 to be choosen in G.

Let $g_1, g_2 \in G$. The following shows that g_1 and g_2 represent the same G/U-coset if and only if they represent the same G_0/U_0-coset

$$g_1U = g_2U \iff g_1^{-1}g_2 \in U \iff g_1^{-1}g_2 \in U_0 \cap G \iff g_1^{-1}g_2 \in U_0\,.$$

As $U^g \subset U_0^g$ for all $g \in G$, it remains to show $G_p \subset U_0^g \Rightarrow G_p \subset U^g$. This is done as follows

$$G_p \subset U_0^g \Longrightarrow G_p \subset U_0^g \cap G \overset{g\in G}{\Longrightarrow} G_p \subset U_0^g \cap G^g \Longrightarrow G_p \subset (U_0 \cap G)^g \Longrightarrow G_p \subset U^g.$$

□

Remarks. The lemma shows that we can solve the short coset problem for $U_0 \subset G_0$ by solving it for the subgroups $U \subset G$. In practice, one needs a source for homomorphisms.

As we deal with permutation groups, it is obvious to take the action on one orbit of an intransitive group. Further, for each orbit, one can take the action on all block systems. Other quotients of G_0 that are easy to handle are the abelian quotient $G_0/[G_0, G_0] = G_0/G_0'$ or G_0/G_0''.

In case we found a good homomorphism that led to a proper subgroup G of G_0, one can repeat the homomorphism search, as the smaller group may have more orbits or other block systems. Further, the iterated treatment of abelian quotients and G_0/G_0'' exhausts the solvable quotient of G_0.

When a further reduction to smaller subgroups is no longer possible, we use the old algorithm to get the short cosets.

5. An Example

Let us inspect the computation of the Galois group of the polynomial $f = t^{63} + t^7 + 128$. The stem field $L := \mathbb{Q}[t]/(f)$ has the obvious subfield $K := \mathbb{Q}[u]/(u^9 + u + 128)$. This is an generic Sym(9) field. From this, we get $\mathrm{Sym}(7) \wr \mathrm{Sym}(9)$ as starting group that contains the Galois group.

The relative extension L/K has the Galois hull $K[\sqrt[7]{u}, \zeta_7]$. Thus, a smaller supergroup of the Galois group is $\mathrm{AGL}_1(\mathbb{F}_7) \wr \mathrm{Sym}(9)$. We take a closer look at

the computation of the short cosets in the descent step between these two wreath products.

A first search for homomorphisms leads to the projection of the wreath products to S_9. As it stays surjective when we restrict to the subgroup, it can be used. Thus, the lemma allows us to replace Sym(9) by the cyclic group $G_{K,p}$ generated by the Frobenius element in the Galois group of K.

Next, we can use the sign homomorphism of Sym(7), which gives us the solvable quotient of the remaining group. Thus, we take

$$\phi\colon \mathrm{Sym}(7) \wr G_{K,p} \longrightarrow \{\pm 1\}^9 \rtimes G_{K,p}$$

to construct an even smaller subgroup for the short coset problem. Finally, we have to compute the conjugacy classes of a group of order 3177120186324 instead of order 147572911771296399360.

The final result is the group

$$\{(x_1,\ldots,x_9) \in \mathbb{F}_7^9 | \sum x_i = 0\} \rtimes ((\mathbb{Z}/7\mathbb{Z})^\star \times \mathrm{Sym}(9)) \ .$$

Here, the condition $\sum x_i = 0$ relates to the fact that the constant term of f is a 7th power. Further, $(\mathbb{Z}/7\mathbb{Z})^\star$ is the Galois group of the 7th cyclotomic field. All the remaining descent steps are done with the direct computation of short cosets as all subgroups are of moderate index.

The computation of the Galois group with MAGMA 2.20 uses 2 GB of memory and takes 850 to 1350 seconds on one core of an Intel Core i7-3770 CPU with 3.4GHz. The variation is a result of random elements in other parts of the algorithm. Using the old short coset algorithm, we need 3.5 GB of memory. Running MAGMA in profile mode shows that we reduce the running time of the short coset function from 680 to 125 seconds.

Finally, note that, as we reach the wreath product $\mathrm{AGL}_1(\mathbb{F}_7) \wr \mathrm{Sym}(9)$ our algorithm replaces a non-solvable group by a solvable one. Thus, more special algorithms can be used.

References

[1] W. Bosma, J. Cannon, and C. Playoust: The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997) 235–265.

[2] H. J. Coutts, M. Quick, and C. M. Roney-Dougal: The primitive permutation groups of degree less than 4096. Communications in Algebra **39** (2011) no. 10, 3526–3546.

[3] J. Dixon, B. Mortimer: Permutation groups. Springer-Verlag, Berlin, New York 1996

[4] A.-S. Elsenhans: Invariants for the computation of intransitive and transitive Galois groups, Journal of Symbolic Computation **47** (2012) 315–326.

[5] C. Fieker, J. Klüners: Computation of Galois Groups of rational polynomials, to appear in: LMS Journal of Computation and Mathematics.

[6] K. Geißler: Berechnung von Galoisgruppen ber Zahl- und Funktionenkörpern, Dissertation, Berlin, 2003.

[7] K. Geißler, J. Klüners: Galois group computation for rational polynomials. In: Algorithmic Methods in Galois Theory. J. Symbolic Comput. **30** (2000) no. 6, 653–674.

[8] B. Huppert: Endliche Gruppen. I. Springer-Verlag, Berlin, New York 1967

[9] J. Leon: Partitions, refinements, and permutation group computation. DIMACS Ser. Discrete Math. Theoret. Comput. Sci., **28** (1997), 123 – 158

[10] R. Stauduhar: The determination of Galois groups. Math. Comp. **27** (1973), 981–996.